

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-272925

(43)公開日 平成8年(1996)10月18日

(51)Int.Cl. [*]	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 K 19/10			G 0 6 K 19/00	R
17/00			17/00	T
19/07			19/00	H

審査請求 未請求 請求項の数4 OL (全9頁)

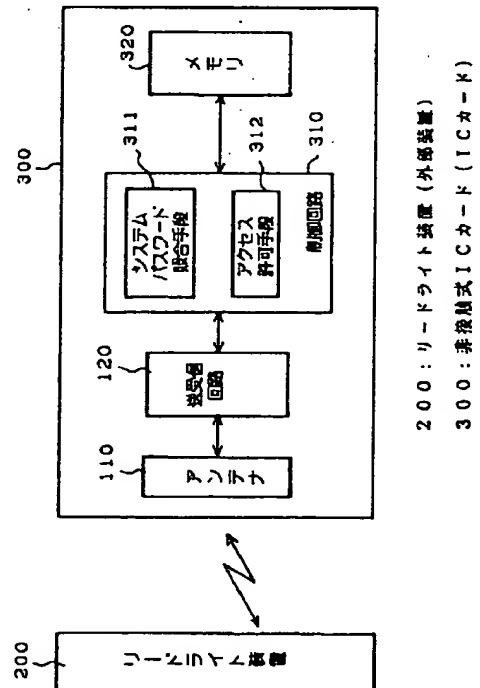
(21)出願番号	特願平7-71778	(71)出願人	000006013 三菱電機株式会社 東京都千代田区丸の内二丁目2番3号
(22)出願日	平成7年(1995)3月29日	(71)出願人	391024515 三菱電機セミコンダクタソフトウエア株式会社 兵庫県伊丹市中央3丁目1番17号
		(72)発明者	藤岡 宗三 伊丹市中央3丁目1番17号 三菱電機セミコンダクタソフトウエア株式会社内
		(74)代理人	弁理士 高田 守 (外4名)

(54)【発明の名称】 ICカード

(57)【要約】

【目的】 テストを容易にできるICカードを提供すること。

【構成】 メモリのシステムエリアにシステムバスワード領域に格納されているシステムバスワードの照合が必要であることを示す第1の情報が格納されている場合にはバスワード照合の結果、バスワードが一致しているときだけ外部装置からのシステムエリアのアクセスを許可する。システムエリアに第1の情報が格納されていない場合にはバスワードの照合なしに外部装置からのアクセスを許可する。



【特許請求の範囲】

【請求項1】 外部装置との間で通信を行うICカードにおいて、システムエリアとユーザエリアとに分割されているメモリであって、前記システムエリアは前記システムエリアを前記外部装置からアクセスするときに照合されるシステムパスワードを格納するためのシステムパスワード格納領域と、前記システムエリアをアクセスする場合に前記システムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第1の情報を格納するためのパスワード情報格納領域とを有するメモリと、前記メモリの前記パスワード情報格納領域に前記第1の情報が格納されている場合には、前記システムエリアを外部からアクセスする際に前記外部装置から送られてくるパスワードと前記システムパスワード格納領域に格納されているシステムパスワードとの照合を行うパスワード照合手段と、前記パスワード情報格納領域に前記第1の情報が格納されている場合には、前記パスワード照合手段の照合の結果パスワードが一致しているときだけ前記外部装置からのアクセスを許可し、前記パスワード情報格納領域に前記第1の情報が格納されていない場合には、パスワードの照合なしに前記外部装置からのアクセスを許可するアクセス許可手段とを具備することを特徴とするICカード。

【請求項2】 前記システムエリアにはさらに前記ユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第2の情報を格納するための拡張システムエリア情報格納領域を有し、前記アクセス許可手段は前記拡張システムエリア情報格納領域に前記第2の情報が格納されている場合には、前記外部装置から前記拡張システムエリアがアクセスされる際に、前記パスワード照合手段の照合の結果、入力されたパスワードが前記システムパスワード格納領域に格納されているシステムパスワードと一致しているときに、前記外部装置からのアクセスを許可することを特徴とする請求項1記載のICカード。

【請求項3】 前記拡張システムエリアは前記ユーザエリアをアクセスする場合に照合されるユーザエリアパスワードを格納するユーザエリアパスワード格納領域を有しており、前記ICカードは、さらに、前記外部装置から前記ユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと前記拡張システムエリアに格納されているユーザエリアパスワードとを照合するユーザエリアパスワード照合手段を有し、前記アクセス許可手段は前記ユーザエリアパスワード照合手段による照合の結果、パスワードが一致した場合には、前記ユーザエリアに対する前記アクセスを許可することを特徴とする請求項2記載のICカード。

【請求項4】 前記ユーザエリアパスワード格納領域には、前記外部装置からリードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワード

と、前記外部装置からライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとが格納され、前記ユーザエリアパスワード照合手段は前記外部装置から入力されるコマンドの種類に基づいて前記リードパスワード、前記ライトパスワードのいずれかとパスワードの照合を行うことを特徴とする請求項3記載のICカード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明はプログラマブルなメモリを有し、電波等でデータ通信を行う非接触式のICカードに関するものである。

【0002】

【従来の技術】 例えば、列車の定期券に非接触式ICカードを用いて、改札口に備えられたリードライト装置との間でデータの転送をすることによって、その定期券が有効であるか否かをチェックするシステムが開発されつつある。

【0003】 図9は従来の非接触式ICカードの構成を示すブロック図である。同図において、100は非接触式ICカード、200は非接触式ICカード100と通信を行うリードライト装置、110はリードライト装置との間で電波の授受を行うために電気信号を電波に変換し、さらに電波を高周波信号に変換するアンテナ、120はアンテナ110によって変換された高周波信号をデジタル信号に変換し、デジタル信号をアンテナ110に供給するための高周波信号に変換する送受信回路、130はデータを格納するメモリ、140は非接触式ICカード100の各部の制御を行うとともに非接触式ICカード100にデータの情報処理等を行う制御回路である。リードライト装置200は非接触式ICカード100に電波によりコマンドを送り非接触式ICカード100はそのコマンドを実行し実行結果をリードライト装置200に返送するように動作する。

【0004】 図10はメモリ130の構成を示す図である。同図に示すようにメモリ130はシステムパスワードを格納する固定メモリ131とシステムエリアとユーザエリアに分割されているプログラマブルメモリ132とから構成されている。リードライト装置200がシステムエリアのアクセスコマンドを非接触式ICカード100に送る場合にはコマンドにシステムパスワードを附加して送る。そして、このパスワードと非接触式ICカード100内の固定メモリ131に格納されているシステムパスワードとを照合し、一致したときのみアクセスできる。このためICカードのメモリのテストを行う際にも、システムエリアのテストはパスワードが必要なためテストが煩わしいという問題があった。さらに固定メモリ131にシステムパスワードが格納されているのでパスワードの変更が難しく、このためパスワードが破られた場合などに、その対応が難しいという問題があった。

【0005】

【発明が解決しようとする課題】従来の非接触式ICカードは、以上のように構成されているので、メモリのテストが煩わしく、さらにパスワードの変更が難しいなどの問題点があった。

【0006】この発明は上記の問題点を解消するためになされたもので、メモリのテストが簡単にできるようになるとともにパスワードの変更も容易にできるICカードを提供することを目的とする。

【0007】

【課題を解決するための手段】請求項1の発明に係るICカードは、システムエリアにシステムエリアを外部装置からアクセスするときに照合されるシステムパスワードを格納するためシステムパスワード格納領域と、システムエリアをアクセスする場合にシステムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第1の情報を格納するためのパスワード情報格納領域とを有するメモリと、パスワード情報格納領域に第1の情報が格納されている場合にはシステムエリアを外部からアクセスする際に外部装置から送られてくるパスワードとシステムパスワード格納領域に格納されているシステムパスワードとの照合を行うパスワード照合手段と、パスワード情報格納領域に第1の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第1の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可するアクセス許可手段とを具備したものである。

【0008】請求項2の発明に係るICカードは、請求項1の発明において、システムエリアにはさらにユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第2の情報を格納するための拡張システムエリア情報格納領域を有し、アクセス許可手段は拡張システムエリア情報格納領域に第2の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可する構成したものである。

【0009】請求項3の発明に係るICカードは、請求項2の発明において、拡張システムエリアはユーザエリアをアクセスする場合に照合されるユーザエリアパスワードを格納するユーザエリアパスワード格納領域を有しており、ICカードは、さらに、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合するユーザエリアパスワード照合手段を有し、アクセス許可手段はユーザ

エリアパスワード照合手段による照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可する構成としたものである。

【0010】請求項4の発明に係るICカードは、請求項3の発明において、ユーザエリアパスワード格納領域には、外部装置からリードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワードと、外部装置からライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとが格納され、ユーザエリアパスワード照合手段は外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行う構成としたものである。

【0011】

【作用】請求項1の発明におけるアクセス許可手段は、パスワード情報格納領域に第1の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第1の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可する。

【0012】請求項2の発明におけるアクセス許可手段は、拡張システムエリア情報格納領域に第2の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可する。

【0013】請求項3の発明におけるユーザエリアパスワード照合手段は、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合し、アクセス許可手段はユーザエリアパスワード照合手段による照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可する。

【0014】請求項4の発明におけるユーザエリアパスワード照合手段は外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行う。

【0015】

【実施例】

実施例1. 次に、この発明の一実施例を図について説明する。図1はこの発明の実施例1の非接触式ICカードの構成を示す図である。なお、図9に示す従来の非接触式ICカードと同一の部分には同一の符号を付し、重複する説明は省略する。図において、300はこの実施例の非接触式ICカード(ICカード)、310は非接触式ICカード300の各部の制御を行うとともにデータの情報処理等を行う制御回路、320はデータを格納す

るためのプログラマブルのメモリである。

【0016】図2はメモリ320のメモリマップを示す図である。同図に示すようにメモリ320はユーザエリアUAとシステムエリアSAとに分けられている。ユーザエリアUAは非接触式ICカード300を使用する人の個人情報や金額データなどアプリケーション用のデータとして使用するエリアである。システムエリアSAは非接触式ICカード300の制御のために使用するエリアである。システムエリアSAには、システムID、カードID、システムパスワード、及びシステムパスワードをシステムエリアSAに対して有効にするためのシステムパスワード有効コード（第1の情報）が格納される。システムパスワード有効コードがシステムパスワード有効コード格納エリアに格納されるとリードライト装置（外部装置）200から非接触式ICカード300のリードライトのアクセスをするコマンドに付加されてきたパスワードがシステムエリアSAに格納されているシステムパスワードと一致した場合にのみシステムエリアのアクセスを行うことができるよう構成されている。

【0017】また、制御回路310にはリードライト装置200からコマンドとともに送られてきたシステムパスワードをメモリ320のシステムエリアSAに格納されているシステムパスワードと比較するシステムパスワード照合手段311、及び、システムエリアSAのシステムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードが格納されており、かつ、送られてきたパスワードとシステムエリアSAに格納されているパスワードとが一致した場合にはリードライト装置200からのアクセスを許可してコマンドを実行するアクセス許可手段312を有している。なお、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コード（例えば、「B9H」）が格納されていない場合には、システムパスワードの照合の結果、パスワードが一致していないてもリードライト装置200からのアクセスは許可される。さらに、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードが格納されていない場合には、リードライト装置200からパスワードなしでコマンドが入力された場合であっても、このコマンドはアクセス許可されて実行されるよう構成されている。

【0018】次に動作について説明する。リードライト装置200が非接触式ICカード300のメモリ320のユーザエリアUAのデータをリードする場合、リードコマンドとリードアドレスとを電波として非接触式ICカード300に送る。非接触式ICカード300はアンテナ110で、送られてきた電波を高周波信号に変換し、送受信回路120で復調及びデコードを実行して制御回路310にリードコマンド及びリードアドレスを転送する。ユーザエリアUAのアクセスにはパスワードの

照合は必要ないのでアクセス許可手段312によりリードコマンドは許可され、メモリ320のリードアドレスに対応するデータが読み出されて、送受信回路120及びアンテナ110を介してリードライト装置200に電波として送出される。

【0019】リードライト装置200からデータを非接触式ICカード300にデータライトをする場合には、ライトコマンド、ライトアドレス、ライトデータを上述したデータのリードと同様にして電波として送出する。

非接触式ICカード300では、データのリードの場合と同様に制御回路310にライトコマンド、ライトアドレス、ライトデータが転送される。ユーザエリアUAのアクセスにはパスワードの照合は必要ないのでアクセス許可手段312によりライトコマンドは許可され、メモリ320のライトアドレスにライトデータが書き込まれる。

【0020】次にこの実施例の特徴的動作であるメモリ320のシステムエリアSAのアクセスについて説明する。リードライト装置200から非接触式ICカード300のシステムエリアSAのリードライトはコマンドにパスワードを付加して非接触式ICカード300に送出する。非接触式ICカード300のシステムパスワード照合手段311は、まず、システムエリアSAのシステムパスワード有効コード格納エリアに特定のコードが格納されているかどうかを確認する。実際には、非接触式ICカード300が起動されるときに制御回路310に設けられているレジスタにシステムパスワード有効コード格納エリアのデータが転送され、このレジスタから出力される信号を参照して特定のコードが格納されているかどうかを確認する。このレジスタ等の構成については後に詳細に説明する。

【0021】システムパスワード有効コード格納エリアに特定のコードが格納されていない場合にはシステムパスワードを付加せずにシステムエリアをアクセスすることができます。従って、リードライト装置200からパスワードを付加せずにコマンドを送るだけで制御回路310のアクセス許可手段312はリード、ライト等のコマンドをユーザエリアUAのアクセスと同様に許可し、実行する。

【0022】非接触式ICカード300の発行前に、メモリ320のテスト等を行う場合にはシステムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードを格納せずにシステムエリアSAをアクセスする。このようにすることでパスワードの照合を行うことなく、システムエリアSAをアクセスすることが可能になる。すなわち、システムパスワード有効コード格納エリアに特定パターンのシステムパスワード有効コードを格納しない場合にはリードライト装置200はシステムエリアSAをユーザエリアUAと同様にアクセスすることが可能になり、テストにかかる時間を短縮す

ることができる。

【0023】特に、メモリ320の製造直後、すなわち、メモリのウェハ工程の終了直後はシステムパスワードが格納される領域の値がどのような値になっているかは不明であるのでシステムパスワードの照合なしにシステムエリアSAをアクセスできるようにすることは重要である。このため、メモリ320のシステムエリアSAのシステムパスワード有効コード格納エリアにはメモリのウェハ工程の終了直後になりやすいコード、「00H」、「01H」、「03H」、「07H」、「0FH」、「1FH」、「3FH」、「7FH」、「FFH」はさけることが望ましい。さらに、テストでメモリに書き込むコード、「00H」、「FFH」、「55H」、「AAH」も避けることが望ましい。この実施例では「B9H」のコードを用いている。

【0024】次に、テストが終了して、実際に非接触式ICカード300が発行される場合には、リードライト装置200等からシステムパスワードの書き込みのコマンドを非接触式ICカード300に送出する。このコマンドに従って、非接触式ICカード300がシステムパスワードをシステムエリアSAにセットした後、リードライト装置200等からシステムパスワード有効コード格納エリアに「B9H」を書き込むコマンドを非接触式ICカード300に送出する。このコマンドが実行されると、システムパスワードは有効になり、リードライト装置200からシステムエリアSAをアクセスする場合には、システムパスワードの照合が必要になる。このため、発行された非接触式ICカード300ではセキュリティが保たれる。また、一旦発行された後でも、システムパスワードを知り得れば、システムパスワードを書き換えることも可能であり、一定期間ごとにシステム全体のパスワードを変更することによって極めて高いセキュリティを得ることが可能になる。

【0025】次に、システムパスワード有効信号について説明する。図3はシステムパスワード有効信号SPEの発生回路を示す回路図である。同図において、314は非接触式ICカード300の起動時にシステムエリアSAのシステムパスワード有効コード格納エリアのデータが転送されて格納される8ビットレジスタ、315はこのレジスタ314が「B9H」になったときに「H」信号を出力するゲートである。非接触式ICカード300が起動される度にレジスタ314にはシステムパスワード有効コード格納エリアのデータがロードされる。そして、システムパスワード有効信号SPEは、システムパスワードが有効な場合にのみ「H」信号を出力する。従って、アクセス許可手段312はこのシステムパスワード有効信号SPEが「L」の場合はシステムエリアSAのアクセスにシステムパスワードの照合が不要であると判断し、「H」の場合は、照合が必要であると判断する。

【0026】図3に示すシステムパスワード有効信号の発生回路では8ビットのレジスタ314を用いたが、図4に示すように、1ビットのレジスタであるフリップフロップ321を用いるようにしても良い。この場合は、非接触式ICカード300の起動時にメモリ320のシステムパスワード有効コード格納エリアのデータをリードし、そのデータが「B9H」であったか否かがフリップフロップ321にセットされる。このフリップフロップ321の出力信号がシステムパスワード有効信号SPEとして用いられる。

【0027】実施例2、図5はこの発明の実施例2の非接触式ICカードの構成を示す図である。なお図1に示す非接触式ICカードと同一の部分には同一の符号を付し、重複する説明は省略する。図において、300aはこの実施例の非接触式ICカード(ICカード)、310aは非接触式ICカード300aの各部の制御を行うとともにデータの情報処理等を行う制御回路である。

【0028】図6はメモリ320のメモリマップを示す図である。なお、図2に示した部分と同一部分には同一の符号を付し、重複する説明は省略する。図6に示すように、メモリ320のアドレス0にはシステムエリアSAが設けられており、このエリアには図2に示すものに加えてシステムエリア拡張コード格納エリアが設けられている。このシステムエリア拡張コード格納エリアにシステムエリア拡張コード(第2の情報)を書き込むことによってアドレス1の拡張システムエリアESAがさらにシステムエリアとして確保されるように構成されている。拡張システムエリアESAには、リードパスワード(ユーザエリアパスワード)、リードパスワードリミットアドレス、ライトパスワード(ユーザエリアパスワード)、ライトパスワードリミットアドレスが格納される。リードパスワード、ライトパスワードは、それぞれ、ユーザエリアをリード、ライトする際に照合されるパスワードである。また、リードパスワードリミットアドレスはリードパスワードが有効となる上限のアドレスを示すものであり、ライトパスワードリミットアドレスはライトパスワードが有効となる上限のアドレスを示すものである。この実施例の場合にはリードパスワードリミットアドレスは10、ライトパスワードリミットアドレスは5となっている。またこの実施例ではシステムパスワード有効コード格納エリアは7ビット、システムエリア拡張コード格納エリアは1ビットの領域となっている。

【0029】図7はシステムパスワード有効信号SPE及びシステム拡張信号SXを生成する回路を示す図である。上述した実施例1では8ビットすべてをシステムパスワード有効コードを格納するために用いたが、この実施例ではB1T1からB1T7までの7ビットに、システムパスワード有効コード格納エリアのデータが、B1T0にはシステムエリア拡張コード格納エリアのデータ

が、それぞれ、非接触式ICカード300aの起動時にロードされる。317はゲートであり、レジスタ314に「B8H」または「B9H」が格納されている場合にシステムパスワード有効信号SPEとして「H」を出力する。さらに、316はゲートであり、レジスタ314に「B9H」が格納されている場合にのみシステム拡張信号SXとして「H」信号を出力する。

【0030】次に、この実施例の動作について説明する。まず、非接触式ICカード300aのシステムエリアSAのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアとの領域に「B8H」を書き込んだ場合には、システム拡張信号SXは「L」信号になり、システムパスワード有効信号SPEは「H」になる。この場合にはアドレス0のシステムエリアSAに対してのみシステムパスワードが有効になる。すなわち、システムエリアSA以外の領域がユーザエリアUA2として使用できる。この場合には実施例1と同様となり、ユーザエリアUA2はパスワードなしでアクセスすることができ、システムエリアSAのアクセスはシステムパスワードの照合が必要になる。

【0031】一方、システムエリアSAのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアとの領域に「B9H」を書き込んだ場合には、システム拡張信号SXとシステムパスワード有効信号SPEのどちらも「H」信号になる。このため、図6に示すように、アドレス1の拡張システムエリアESAとシステムエリアSAのどちらに対してもシステムエリアSAに格納されているシステムパスワードが有効になる。すなわち、アクセス許可手段312はシステム拡張信号SX及びシステムパスワード有効信号SPEに基づいてシステムパスワード照合手段311によるシステムパスワードの照合が必要になるか否かを判断する。

【0032】さらに、拡張システムエリアESAが確保された場合には、ユーザエリアUA1は、拡張システムエリアESAに格納されるリードパスワード、リードパスワードリミットアドレス、ライトパスワード、ライトパスワードリミットアドレスを用いて、ユーザエリアパスワード照合手段313によってパスワードの照合が行われ、アクセス許可手段312によってパスワードとともにに入力されたコマンドが許可されるか否かが判断される。ユーザエリアUA1はアドレス2から15までであるので、ライトパスワードの有効エリアはアドレス2から10、リードパスワードの有効エリアはアドレス2から5になる。すなわち、アドレス2から5までのエリアはリード、ライトともにパスワードが必要になる。従って、このエリアには金額等の機密性の高いデータで発行後もリードライトすることが必要なデータを格納するのに適する。また、アドレス6から10まではリードについてのみパスワードが必要になる。このため、住所、氏名、電話番号など発行後は読み出しだけですむデータを

格納するのに適する。さらにアドレス11から15まではパスワードなしでアクセスすることが可能である。このため、セキュリティ不要のデータを格納するのに適する。このように、ライトパスワード、リードパスワードの2つのパスワードを設けることで、セキュリティのレベルの異なる3種類の領域に分割して管理することができる。また、リミットアドレスを変更することにより、それぞれの領域の大きさを変更することができ、メモリを効率よく管理して使用することができる。

【0033】なお、図7では、システム拡張信号SXとシステムパスワード有効信号SPEを生成するのに8ビットのレジスタ314を用いたが、図8に示すように1ビットのレジスタであるフリップフロップ318、319を用いて図4に示した場合と同様に出力されるシステム拡張信号SXとシステムパスワード有効信号SPEを直接ラッチするようにも良い。

【0034】なお、システムエリアSAのシステムパスワード有効コード格納エリアとシステムエリア拡張コード格納エリアに「B9H」、「B8H」以外のデータが格納されていた場合には、リードライト装置200から入力されたコマンドはパスワードの照合なしで実行される。

【0035】以上のように、この実施例では、拡張システムエリアをユーザエリアに確保できるとともに、ユーザエリアをリードパスワードとライトパスワードを用いてセキュリティを高くしてアクセスの管理を行うことができる。

【0036】

【発明の効果】請求項1記載の発明によれば、パスワード情報格納領域にシステムパスワード領域に格納されているシステムパスワードの照合が必要であることを示す第1の情報が格納されている場合にはパスワード照合手段の照合の結果パスワードが一致しているときだけ外部装置からのアクセスを許可し、パスワード情報格納領域に第1の情報が格納されていない場合にはパスワードの照合なしに外部装置からのアクセスを許可するように構成したので、ICカードのテストなどのときにはパスワードなしにアクセスできるのでテスト等の時間を短縮することができる効果がある。

【0037】請求項2記載の発明によれば、拡張システムエリア情報格納領域に、ユーザエリア内の所定の大きさの領域を拡張システムエリアとして使用することを示す第2の情報が格納されている場合には、外部装置から拡張システムエリアがアクセスされる際にはパスワード照合手段の照合の結果、入力されたパスワードがシステムパスワード格納領域に格納されているシステムパスワードと一致しているときに外部装置からのアクセスを許可するように構成したので、システムパスワードの有効となる範囲を可変することができ、多種のシステムに対応することができる効果がある。

【0038】請求項3記載の発明によれば、外部装置からユーザエリアに対してパスワードとともにアクセスがあった場合に、このパスワードと拡張システムエリアに格納されているユーザエリアパスワードとを照合し、照合の結果、パスワードが一致した場合には、ユーザエリアに対するアクセスを許可するように構成したので、ユーザエリアに対してもパスワードの照合によってセキュリティを向上させることができる効果がある。

【0039】請求項4記載の発明によれば、ユーザエリアパスワード格納領域には、リードコマンドがパスワードとともに送られてきた場合に照合されるリードパスワードと、ライトコマンドがパスワードとともに送られてきた場合に照合されるライトパスワードとを格納し、外部装置から入力されるコマンドの種類に基づいてリードパスワード、ライトパスワードのいずれかとパスワードの照合を行うように構成したので、コマンドの種類に基づいて、効果的にユーザエリアをセキュリティ高く管理することができる効果がある。

【図面の簡単な説明】

【図1】この発明の実施例1の非接触式ICカードの構成を示す図である。

【図2】図1に示す非接触式ICカードのメモリのメモリマップを示す図である。

【図3】実施例1における、8ビットのレジスタを用*

*いたシステムパスワード有効信号の発生回路を示す図である。

【図4】実施例1における、1つのフリップフロップを用いたシステムパスワード有効信号の発生回路を示す図である。

【図5】この発明の実施例2の非接触式ICカードの構成を示す図である。

【図6】図5に示す非接触式ICカードのメモリのメモリマップを示す図である。

【図7】実施例2における、8ビットのレジスタを用いたシステムパスワード有効信号及びシステム拡張信号を生成する回路を示す図である。

【図8】実施例2における、2つのフリップフロップを用いたシステムパスワード有効信号及びシステム拡張信号を生成する回路を示す図である。

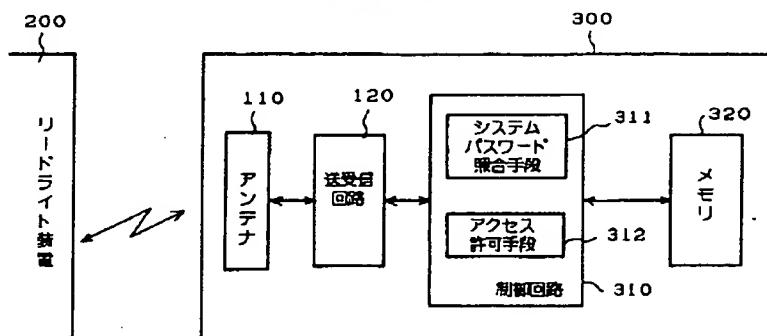
【図9】従来の非接触式ICカードの構成を示すブロック図である。

【図10】図9に示すメモリの構成を示す図である。

【符号の説明】

200 リードライト装置（外部装置）、300、300a 非接触式ICカード（ICカード）、312 アクセス許可手段、313 ユーザエリアパスワード照合手段、320 メモリ。

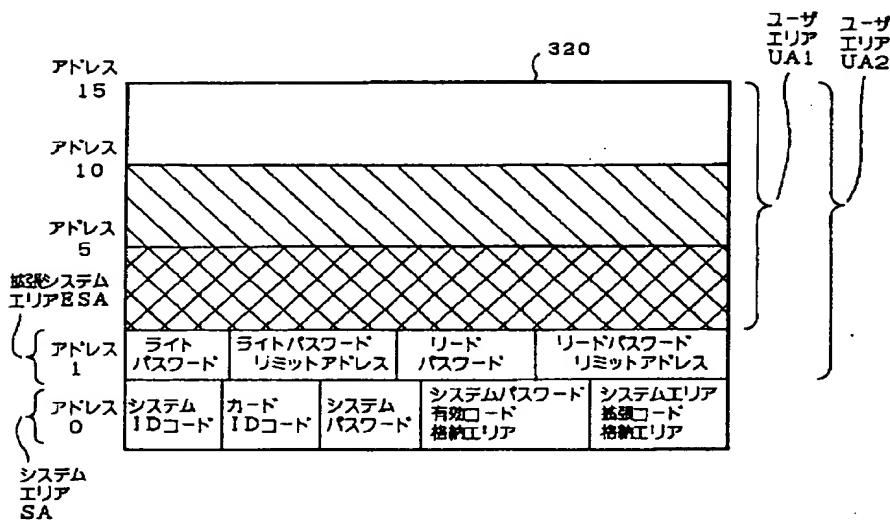
【図1】



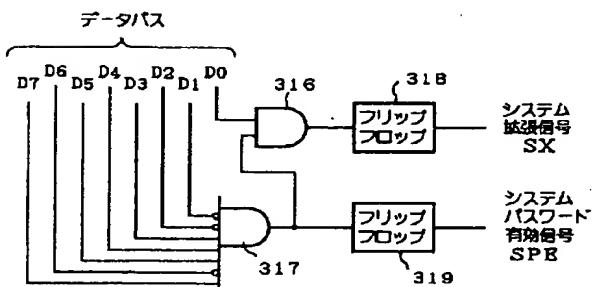
200: リードライト装置（外部装置）

300: 非接触式ICカード（ICカード）

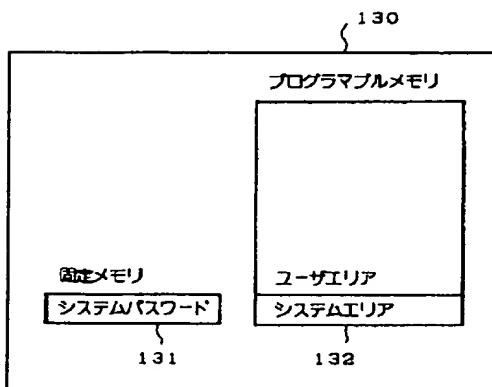
【図6】



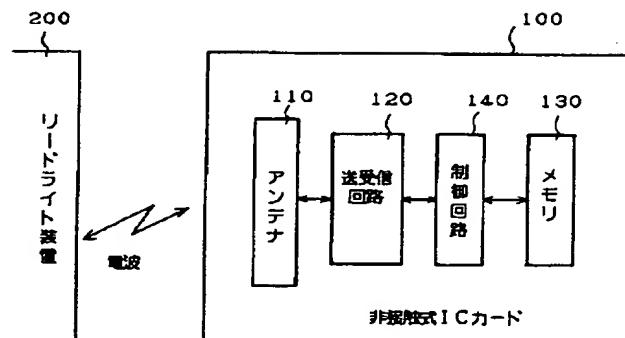
【図8】



【図10】



【図9】





Creation date: 11-15-2004

Indexing Officer: ZBANGURA - ZAIN BANGURA

Team: OIPEBackFileIndexing

Dossier: 09635217

Legal Date: 01-20-2004

No.	Doccode	Number of pages
1	RCEX	1
2	A...	1
3	CLM	6
4	REM	4
5	XT/	1

Total number of pages: 13

Remarks:

Order of re-scan issued on